



September 2015

# DEFENSE CYBERSECURITY

## Opportunities Exist for DOD to Share Cybersecurity Resources with Small Businesses

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE <b>SEP 2015</b>		2. REPORT TYPE		3. DATES COVERED <b>00-00-2015 to 00-00-2015</b>	
4. TITLE AND SUBTITLE <b>Defense Cybersecurity: Opportunities Exist for DOD to Share Cybersecurity Resources with Small Businesses</b>				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) <b>U.S. Government Accountability Office,,441 G Street NW, Room 7149,Washington,,DC, 20548</b>				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT <b>Approved for public release; distribution unlimited</b>					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT <b>Same as Report (SAR)</b>	18. NUMBER OF PAGES <b>33</b>	19a. NAME OF RESPONSIBLE PERSON
a REPORT <b>unclassified</b>	b ABSTRACT <b>unclassified</b>	c THIS PAGE <b>unclassified</b>			

# GAO Highlights

Highlights of [GAO-15-777](#), a report to congressional committees

## Why GAO Did This Study

Small businesses, including those that conduct business with DOD, are vulnerable to cyber threats and may have fewer resources, such as robust cybersecurity systems, than larger businesses to counter cyber threats.

The Joint Explanatory Statement accompanying the National Defense Authorization Act for Fiscal Year 2015 included a provision that GAO assess DOD OSBP's outreach and education efforts to small businesses on cyber threats. This report addresses the extent to which DOD OSBP has integrated cybersecurity into its outreach and education efforts to defense small businesses. DOD OSBP's mission includes providing small business policy advice to the Office of the Secretary of Defense, and policy oversight to DOD military department and component small business offices.

To conduct this review, GAO analyzed documentation and interviewed officials from DOD OSBP about its cybersecurity outreach and education efforts. GAO also analyzed documentation and interviewed officials from nine organizations selected for their cybersecurity expertise to identify examples of cybersecurity outreach and education programs potentially available to defense small businesses.

## What GAO Recommends

GAO recommends that DOD identify and disseminate cybersecurity resources to defense small businesses. DOD concurred with the recommendation and agreed to implement training events and education programs.

View [GAO-15-777](#). For more information, contact Joseph W. Kirschbaum at (202) 512-9971 or [kirschbaumj@gao.gov](mailto:kirschbaumj@gao.gov).

September 2015

## DEFENSE CYBERSECURITY

### Opportunities Exist for DOD to Share Cybersecurity Resources with Small Businesses

## What GAO Found

The Department of Defense (DOD) Office of Small Business Programs (OSBP) has explored some options, such as online training videos, to integrate cybersecurity into its existing efforts; however, as of July 2015, the office had not identified and disseminated cybersecurity resources in its outreach and education efforts to defense small businesses. While DOD OSBP is not required to educate small businesses on cybersecurity, DOD OSBP officials acknowledged that cybersecurity is an important and timely issue for small businesses—and therefore the office is considering incorporating cybersecurity into its existing outreach and education efforts. During the review, GAO identified 15 existing federal cybersecurity resources that DOD OSBP could disseminate to defense small businesses.

#### Selected Examples of Cybersecurity Resources GAO Identified as Available to Defense Small Businesses

Resource	Implementing Agency	Program Overview
<a href="#">Cybersecurity e-Learning Courses</a>	DOD Defense Security Service	Online courses related to cybersecurity topics such as risk management and phishing—that is, social engineering that uses authentic-looking, but fake, e-mails to request information from users or direct them to a fake website that requests information.
<a href="#">Cybersecurity for Small Business</a>	U.S. Small Business Administration	Provides a 30 minute online program that covers cybersecurity concepts for small business.
<a href="#">Small Biz Cyber Planner 2.0</a>	Federal Communications Commission	Provides guidance based on areas of risk self-identified by small businesses. The guidance includes links to additional cybersecurity resources for small businesses.

Source: GAO analysis of information from listed agencies. | GAO-15-777

While DOD OSBP officials recognized the importance of identifying and disseminating cybersecurity resources through outreach and education efforts to small businesses, they identified factors that had limited their progress in doing so. Specifically, they were not aware of existing cybersecurity resources, they had leadership turnover in the office, and the office was focused on developing a training curriculum for professionals who work with small businesses. While GAO recognizes that these factors could affect progress, federal government internal controls state that management should ensure there are adequate means of communicating with, and obtaining information from, external stakeholders who may have a significant impact on the agency's achieving its goals. DOD OSBP officials agreed that identifying and disseminating information about existing cybersecurity resources to defense small businesses could help small businesses be more aware of cybersecurity practices and cyber threats. In addition, by identifying and disseminating this information, DOD OSBP could help small businesses to protect their networks, thereby supporting the 2015 DOD Cyber Strategy goals of working with the private sector to help secure defense industrial base trade data and build layered cyber defenses.

---

# Contents

---

Letter		1
	Background	4
	DOD Office of Small Business Programs Had Not Identified and Disseminated Cybersecurity Resources to Defense Small Businesses	10
	Conclusions	13
	Recommendation for Executive Action	13
	Agency Comments and Our Evaluation	13
Appendix I	Scope and Methodology	16
Appendix II	Federal Government and Federally-Funded Cybersecurity Resources GAO Identified as Available to Defense Small Businesses	19
Appendix III	Comments from the Department of Defense	24
Appendix IV	GAO Contact and Staff Acknowledgments	26
Related GAO Products		27
Tables		
	Table 1: Sources of Cybersecurity Threats	5
	Table 2: Types of Cyber Exploits	6
	Table 3: Cybersecurity Resources GAO Identified as Available to Defense Small Businesses	19

---

## Abbreviations

DOD	Department of Defense
OSBP	Office of Small Business Programs

---

---

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



September 24, 2015

The Honorable John McCain  
Chairman  
The Honorable Jack Reed  
Ranking Member  
Committee on Armed Services  
United States Senate

The Honorable Mac Thornberry  
Chairman  
The Honorable Adam Smith  
Ranking Member  
Committee on Armed Services  
House of Representatives

The Department of Defense (DOD) depends on small businesses to support its missions, spark innovation, and develop technologies to support the warfighter.<sup>1</sup> In 2014, an official from the Federal Bureau of Investigation testified that businesses are increasingly targeted for theft of trade secrets and economic espionage by foreign entities—often with state sponsorship and backing—that are enabled by cyber intrusions.<sup>2</sup> The Defense Security Service also reported in 2012 that our national security relies on success in thwarting persistent attacks—including cyber attacks—that target U.S. technology, intellectual property, trade secrets and proprietary information.<sup>3</sup> In February 2015, the Director of National Intelligence reported that cyber threats to U.S. national and economic security are increasing in frequency, scale, sophistication, and severity of

---

<sup>1</sup>DOD defines small businesses according to the North American Industry Classification System used by the U.S. Small Business Administration. The North American Industry Classification System assigns codes to economic activity within 20 broad sectors such as Manufacturing, Finance and Insurance, and Educational Services. The codes reflect the industries in which the firms operate, for example wireless telecommunications carriers or industrial building construction.

<sup>2</sup>Randall C. Coleman, Assistant Director, Counterintelligence Division, Federal Bureau of Investigation, *Statement Before the Committee on the Judiciary, Subcommittee on Crime and Terrorism, United States Senate*, May 13, 2014.

<sup>3</sup>Defense Security Service, *Targeting U.S. Technologies 2012, A Trend Analysis of Reporting from Defense Industry*, 2012.

---

impact. He further stated that the range of cyber threat actors, methods of attack, targeted systems, and victims is expanding.<sup>4</sup> Small businesses in particular have fewer resources, such as robust cybersecurity systems, than larger businesses have to counter such threats.<sup>5</sup>

In fiscal year 2014, DOD obligated approximately \$55.5 billion to small business prime contractors at over 51,000 locations.<sup>6</sup> DOD maintains an Office of Small Business Programs (OSBP) to ensure that small businesses receive a fair proportion of DOD purchases, contracts, and subcontracts for property and services.<sup>7</sup> This office, among other things, is responsible for providing small business policy advice to the Office of the Secretary of Defense and for providing policy oversight to DOD military department and DOD component small business offices. These offices are responsible for ensuring that small businesses are afforded the maximum practicable opportunity to participate in DOD acquisitions, as well as establishing challenging small business program goals.

The Joint Explanatory Statement to accompany the National Defense Authorization Act for Fiscal Year 2015 included a provision that GAO assess the DOD OSBP's outreach and education efforts to assist small businesses in understanding cyber threats.<sup>8</sup> This report addresses the extent to which DOD OSBP has integrated cybersecurity into its existing outreach and education efforts for defense small businesses.

We focused our review on DOD OSBP because that office is responsible for providing small business policy advice to the Office of the Secretary of

---

<sup>4</sup>Director of National Intelligence, Statement for the Record, *Worldwide Threat Assessment of the US Intelligence Community*, Senate Armed Services Committee, Feb. 26, 2015.

<sup>5</sup>According to the National Institute of Standards and Technology, cybersecurity is the ability to protect or defend the use of cyberspace from cyber attacks. A threat is the potential source of an adverse event. See NISTIR 7298, Revision 2, *Glossary of Key Information Security Terms*, May 2013.

<sup>6</sup>The source of these data is the Federal Procurement Data System-Next Generation. The Federal Procurement Data System-Next Generation does not identify subcontracted vendors who may also be small businesses that received funds through DOD obligations to prime contractors.

<sup>7</sup>DOD Directive 4205.01 *DOD Small Business Programs* (March 10, 2009).

<sup>8</sup>See Joint Explanatory Statement to accompany the National Defense Authorization Act for Fiscal Year 2015, 160 Cong. Rec. H8700 (Dec. 4, 2014).

---

Defense and providing policy oversight to DOD military department and DOD component small business offices, per DOD Directive 4205.01.<sup>9</sup> While other DOD components may interact with small businesses, such as the DOD Chief Information Officer and military department small business program offices, we found that these other components either do not exclusively focus their efforts on small businesses or, alternatively, they rely on DOD OSBP policy and guidance with regard to working with small businesses. To address our objective, we analyzed documentation and interviewed officials from DOD OSBP about its existing cybersecurity outreach and education efforts to small businesses. We also discussed with DOD OSBP officials any challenges or limitations to their ability to conduct cybersecurity outreach and education. As part of this review, we evaluated the office's efforts by comparing information on its activities with *Standards for Internal Control in the Federal Government*.<sup>10</sup> By reviewing agency websites, interviewing agency officials, and searching literature on cybersecurity resources, we determined that there was no central repository of federal cybersecurity resources that could be leveraged by the DOD OSBP to share with defense small businesses. In the absence of such a central repository, we reviewed documentation and interviewed officials from the following organizations with cybersecurity expertise: DOD Chief Information Officer, Defense Security Service, Defense Information Systems Agency, Department of Homeland Security National Protection and Programs Directorate, Federal Bureau of Investigation Cyber Division, National Institute of Standards and Technology, U.S. Small Business Administration, Federal Communications Commission, and the National Cyber Security Alliance in order to identify examples of existing cybersecurity outreach and education programs potentially available to defense small businesses that could be leveraged by the DOD OSBP. We limited the scope of our research to cybersecurity outreach and education programs that were managed or funded by federal agencies. To confirm that these resources were accessible to defense small businesses, we visited the websites where these resources were publicly available during May 2015 or interviewed agency officials. To validate the relevance of these resources to cybersecurity, we reviewed information on the resource websites to confirm that each resource contained some level of cybersecurity

---

<sup>9</sup>DOD Directive 4205.01 *DOD Small Business Programs*, (March 10, 2009).

<sup>10</sup>GAO, *Standards for Internal Control in the Federal Government*, [GAO/AIMD-00-21.3.1](#) (Washington, D.C.: Nov. 1, 1999).

---

information. We may not have identified all of the resources available or interviewed all knowledgeable parties and we did not assess the quality of the selected resources.

We conducted this performance audit from February 2015 to September 2015 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. See appendix I for a detailed description of the scope and methodology for this report.

---

## Background

---

### Cyber Threats to Federal Government Contractors

Federal government contractors, including defense small businesses, face an evolving array of cyber-based threats. As we testified in April 2015, risks to cyber-based assets can originate from both unintentional and intentional threats.<sup>11</sup> Unintentional threats can be caused by, among other things, defective computer or network equipment, and careless or poorly trained employees. Intentional threats include both targeted and untargeted attacks from a variety of sources, including criminal groups, hackers, disgruntled employees, foreign nations engaged in espionage and information warfare, and terrorists.

Threat sources vary in terms of the capabilities of the actors, their willingness to act, and their motives, which can include monetary gain or political advantage, among others. For example, adversaries possessing sophisticated levels of expertise and significant resources to pursue their objectives—sometimes referred to as “advanced persistent threats”—pose increasing risks. Table 1 presents various sources of cyber threats.<sup>12</sup>

---

<sup>11</sup>GAO, *Cybersecurity: Actions Needed to Address Challenges Facing Federal Systems*, [GAO-15-573T](#) (Washington, D.C.: Apr. 22, 2015).

<sup>12</sup>As described in [GAO-15-573T](#) and GAO, *Insider Threats: DOD Should Strengthen Management and Guidance to Protect Classified Information and Systems*, [GAO-15-544](#) (Washington, D.C.: Jun. 02, 2015).

**Table 1: Sources of Cybersecurity Threats**

Threat source	Description
Bot-net operators	Bot-net operators use a network, or bot-net, of compromised, remotely controlled systems to coordinate attacks and distribute phishing schemes, spam, and malware attacks.
Criminal groups	Criminal groups seek to attack systems for monetary gain. Specifically, organized criminal groups use cyber exploits to commit identity theft, online fraud, and computer extortion. International corporate spies and criminal organizations also pose a threat to the United States through their ability to conduct industrial espionage and large-scale monetary theft and to hire or develop hacker talent.
Hackers/hacktivists	Hackers break into networks for the challenge or for revenge, stalking, or monetary gain, among other reasons. Hacktivists are ideologically-motivated actors who use cyber exploits to further political goals. Although gaining unauthorized access once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus, while attack tools have become more sophisticated, they have also become easier to use. According to the Central Intelligence Agency, the large majority of hackers do not have the requisite expertise to threaten difficult targets such as critical U.S. networks. Nevertheless, the worldwide population of hackers poses a relatively high threat of an isolated or brief disruption causing serious damage.
Insiders	Insiders with access to an organization's information and systems may be able to conduct far more malicious activity—wittingly or unwittingly—than outsiders can, with potentially devastating consequences for the organization. Insiders have an advantage over others who may want to harm an organization because insiders may have an awareness of their organization's vulnerabilities, such as loosely enforced policies and procedures, or exploitable technical flaws. Insiders may not need a great deal of knowledge about computer intrusions because their position within the organization often allows them to gain unrestricted access and cause damage to the targeted system or to steal system data. Even insiders who do not intend to cause harm may inadvertently do so through human error, such as when careless or poorly trained employees inadvertently introduce malware into systems.
Nations	Nations use cyber tools as part of their information-gathering and espionage activities. In addition, several nations are aggressively working to develop information warfare doctrine, programs, and capabilities. Such capabilities enable a single entity to potentially have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power—impacts that could affect the daily lives of citizens across the country. In his February 2015 testimony, the Director of National Intelligence stated that, among state actors, China and Russia have highly sophisticated cyber programs, while Iran and North Korea have lesser technical capabilities but possibly more disruptive intent.
Terrorists	Terrorists seek to destroy, incapacitate, or exploit critical infrastructures in order to threaten national security, cause mass casualties, weaken the economy, and damage public morale and confidence. Terrorists may use cyber exploits in order to generate funds or gather sensitive information.

Source: GAO analysis. | GAO-15-777

Threat sources make use of various techniques—or exploits—that may adversely affect information computers, software, networks, and operations. Table 2 presents various types of cyber exploits.<sup>13</sup> The number of information security incidents reported by federal agencies to the U.S. Computer Emergency Readiness Team increased from 5,503 in

<sup>13</sup>As described in [GAO-15-573T](#).

fiscal year 2006 to 67,168 in fiscal year 2014, an increase of 1,121 percent.<sup>14</sup>

**Table 2: Types of Cyber Exploits**

Type of exploit	Description
Cross-site scripting	An attack that uses third-party web resources to run script—a data file or portion of a data file—within the victim’s web browser or scriptable application. This occurs when a browser visits a malicious website or clicks a malicious link. The most dangerous consequences occur when this method is used to exploit additional vulnerabilities that may permit an attacker to steal cookies (data exchanged between a web server and a browser), log key strokes, capture screen shots, discover and collect network information, or remotely access and control the victim’s machine.
Denial-of-service/distributed denial-of-service	An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources. A distributed denial-of-service attack is a variant of the denial-of-service attack that uses numerous hosts to perform the attack.
Malware	Malware, also known as malicious code or malicious software, refers to a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim’s data, applications, or operating system or otherwise annoying or disrupting the victim. Examples of malware include logic bombs, Trojan Horses, ransomware, viruses, and worms.
Phishing/spear phishing	A digital form of social engineering that uses authentic-looking, but fake, e-mails to request information from users or direct them to a fake website that requests information. Spear phishing is a phishing exploit that is targeted to a specific individual or group.
Passive wiretapping	The monitoring or recording of data, such as passwords transmitted in clear text, while they are being transmitted over a communications link. This is done without altering or affecting the data.
Spamming	Sending unsolicited commercial e-mail advertising for products, services, or websites. Spam can also be used as a delivery mechanism for malware and other cyber threats.
Spoofing	Creating a fraudulent website to mimic an actual, well-known website run by another party. E-mail spoofing occurs when the sender address and other parts of an e-mail header are altered to appear as though the e-mail originated from a different source.
Structured query language injection	An attack that involves the alteration of a database search in a web-based application, which can be used to obtain unauthorized access to sensitive information in a database.
War driving	Driving a vehicle through cities or neighborhoods with a wireless-equipped computer—sometimes with a powerful antenna—searching for unsecured wireless networks.

<sup>14</sup>The United States Computer Emergency Readiness Team works to improve the nation’s cybersecurity posture, coordinate cyber information sharing, and manage cyber risks to the nation as the 24-hour operational arm of the Department of Homeland Security’s National Cybersecurity and Communications Integration Center.

Type of exploit	Description
Zero-day exploit	An exploit that takes advantage of a security vulnerability previously unknown to the general public. In many cases, the exploit code is written by the same person who discovered the vulnerability. By writing an exploit for the previously unknown vulnerability, the attacker creates a potent threat since the compressed timeframe between public discoveries of both makes it difficult to defend against.

Source: GAO analysis. | GAO-15-777

## DOD OSBP's Roles and Responsibilities

DOD has tasked DOD OSBP with ensuring that small businesses receive a fair proportion of DOD purchases, contracts, and subcontracts for property and services.<sup>15</sup> This office is responsible for providing small business policy advice to the Office of the Secretary of Defense and for providing policy oversight to DOD military department and DOD component small business offices. Those offices are responsible for ensuring that small businesses are afforded the maximum practicable opportunity to participate in DOD acquisitions and establishing challenging small business program goals. DOD Directive 4205.01 states that DOD OSBP should take part in outreach and education on small business issues within DOD. Specifically, the directive states that DOD OSBP should establish and support a small business training program for Small Business Specialists and other acquisition personnel within DOD. In addition, DOD OSBP provides resources on the DOD OSBP website, and according to DOD OSBP officials, DOD OSBP also supports small businesses by providing outreach and education by attending small business conferences. However, according to DOD OSBP officials, none of those responsibilities requires the office to integrate cybersecurity into current or new outreach and education efforts.

## Other DOD Components Supporting Small Businesses

While DOD OSBP is responsible for leading DOD's efforts to support small business initiatives, other DOD components support defense small businesses. For example,

- Military department small business office officials told us that their offices routinely provide outreach and education to small businesses on topics such as how to bid on DOD contracts; however, these efforts do not include outreach and education on cybersecurity issues.

<sup>15</sup>DOD Directive 4205.01.

- 
- DOD Chief Information Officer manages the Defense Industrial Base Cyber Security/Information Assurance Program to address the pressing need to stem the risk posed by cyber attacks against defense industrial base businesses.<sup>16</sup> According to DOD Instruction 5205.13, the program established a comprehensive approach for protecting unclassified DOD information transiting or residing on unclassified defense industrial base information systems and networks by incorporating the use of intelligence, operations, policies, standards, information sharing, expert advice and assistance, incident response, reporting procedures, and cyber intrusion damage assessment solutions to address a cyber advanced persistent threat.<sup>17</sup> It was designed to establish a voluntary framework to prevent unauthorized access to DOD program information or the intellectual property of industry. This program is available only to a subset of small companies since participating companies must be approved to maintain classified information.
  - The Defense Security Service manages the National Industrial Security Program for the Undersecretary of Defense for Intelligence, which governs cleared contractor companies and their cleared employees who support DOD and other federal agencies. The Defense Security Service has security oversight of these contractors, and provides them with related counterintelligence services and security education, awareness, and training; this includes the foreign threat to cleared contractors as an aspect of the counterintelligence mission. DOD has designated the Defense Security Service as its provider of security professional training and security awareness products for DOD personnel and for the cleared contractors. Under the National Industrial Security Program, the Defense Security Service receives, analyzes, and shares information on activity involving cleared contractor's networks, regardless of the classification that may reflect foreign intelligence interests and acts in

---

<sup>16</sup>In August 2012, GAO issued a For Official Use Only report that assessed this program and identified opportunities that DOD could take to improve the program. DOD has taken steps to implement some of the report's recommendations. GAO, *Defense Cyber Efforts: Management Improvements Needed to Enhance Programs Protecting the Defense Industrial Base from Cyber Threats*, GAO-12-762SU (Washington, D.C.: Aug. 3, 2012).

<sup>17</sup>According to DOD Instruction 5205.13, *Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA) Activities* (Jan. 29, 2010) an advanced persistent threat is an extremely proficient, patient, determined, and capable adversary, including two or more such adversaries working together.

---

close coordination with the Federal Bureau of Investigation and other federal law enforcement and counterintelligence community members.

---

## Cybersecurity Provision within the Defense Federal Acquisition Regulation Supplement

In November 2013, DOD updated its Defense Federal Acquisition Regulation Supplement to include a contract clause that requires defense contractors and subcontractors to safeguard unclassified controlled technical information on their unclassified information systems from unauthorized access and disclosure and to report certain cyber incidents to DOD.<sup>18</sup> In addition, under the required clause, contractors are to implement minimum privacy and security controls such as risk assessments that were developed by the National Institute of Standards and Technology, among other requirements.<sup>19</sup> The 2015 DOD Cyber Strategy states that DOD must work with the private sector to help secure defense industrial base trade data. Furthermore, to safeguard critical programs and technologies, the strategy states that DOD will work with companies to develop alert capabilities and build layered cyber defenses.<sup>20</sup>

---

<sup>18</sup>See Defense Federal Acquisition Regulation Supplement, §204.7302 and §252.204-7012. Controlled technical information means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. This falls within the general category of Controlled Unclassified Information, which DOD defines as “unclassified information that requires safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulations, and Government-wide policies.” See DOD, Manual 5200.01, Volume 1, *DOD Information Security Program: Overview, Classification, and Declassification* (Feb. 24, 2012).

<sup>19</sup>In August 2015, DOD issued an interim rule amending Defense Federal Acquisition Regulation Supplement §252.204-7012 to require privacy and security controls identified in NIST Special Publication 800-171, rather than the controls from NIST Special Publication 800-53. In addition, the interim rule expands the protection and reporting to entire contractor systems as well as a new type of information—covered defense information—which includes controlled technical information as a subset. See 80 Fed. Reg. 165, 51739-51748 (Aug. 26, 2015). See NIST, *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53 (Gaithersburg MD, April 2013) and NIST, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*, Special Publication 800-171 (Gaithersburg MD, June 2015).

<sup>20</sup>DOD, *The Department of Defense Cyber Strategy* (April 2015).

---

## DOD Office of Small Business Programs Had Not Identified and Disseminated Cybersecurity Resources to Defense Small Businesses

DOD OSBP officials have explored some ways whereby the office could integrate cybersecurity into its existing outreach and education efforts; however, as of July 2015, the office had not identified and disseminated information about cybersecurity resources in its outreach and education efforts to defense small businesses. While DOD OSBP is not required to educate small businesses on cybersecurity, DOD OSBP officials acknowledged that cybersecurity is an important and timely issue for small businesses—and therefore the office is considering incorporating cybersecurity into its existing outreach and education efforts. In response to our review, DOD OSBP officials contacted DOD Chief Information Officer officials in April 2015 to discuss options for integrating cybersecurity into their existing outreach and education efforts. According to DOD OSBP officials, the DOD OSBP and DOD Chief Information Officer officials discussed the development of training materials, such as online videos and brochures that could be distributed at small business conferences. The purpose of such training materials would be to help defense small businesses in understanding cybersecurity best practices, and the cybersecurity requirements identified in the Defense Federal Acquisition Regulation Supplement.<sup>21</sup> According to DOD OSBP officials, the office also invited a DOD Chief Information Officer official to join a DOD OSBP representative to speak with small businesses about cybersecurity and to distribute a handout on cybersecurity and cyber business opportunities at a small business conference held in April 2015. In addition, recognizing that DOD's small business offices may not be staffed by cybersecurity experts, DOD OSBP officials stated that they plan to add a cybersecurity component to a training curriculum that they are currently developing along with DOD Chief Information Officer for professionals who work in DOD small business offices. However, these efforts have not been completed and, as of July 2015, DOD OSBP had not identified or disseminated cybersecurity resources to defense small businesses that the businesses could use to understand cybersecurity and cyber threats.

---

<sup>21</sup>The Defense Federal Acquisition Regulation Supplement §252.204-7012 includes minimum required security controls for unclassified controlled technical information such as access controls and identification and authentication and procedures for cyber incident and compromise reporting, including the contract involved, type of compromise and description of technical information compromised.

---

We identified 15 existing federal cybersecurity outreach and education resources that the office could leverage for defense small businesses.<sup>22</sup> For example:

- DOD's Defense Security Service offers online cybersecurity training programs that are available to the public on topics such as cybersecurity awareness, the National Institute of Standards and Technology's Risk Management Framework,<sup>23</sup> insider threats, and security controls through its public website. According to Defense Security Service officials, DOD small businesses could use the online training programs to improve their knowledge of cybersecurity.
- The U.S. Small Business Administration maintains a learning center that provides a 30-minute online program—available to small businesses—that covers cybersecurity concepts for small business. Topics include identifying and securing sensitive information, types of cyber threats, risk management, and best practices for guarding against cyber threats.
- The Department of Homeland Security, in coordination with the National Cyber Security Alliance and the Anti-Phishing Working Group, provides cyber awareness resources to the public—including cybersecurity awareness videos and tip sheets—on its Stop.Think.Connect website and facilitates cybersecurity awareness events targeted to various audiences, including businesses. This resource is available to defense small businesses.
- The Federal Communications Commission hosts a planning tool on its website, known as the FCC Small Biz Cyber Planner 2.0 that is targeted to small businesses and available to the public. This online planner provides guidance to small businesses on developing their cybersecurity plans and is available to defense small businesses.

---

<sup>22</sup>Appendix II provides a listing of selected federal cybersecurity resources, including public cybersecurity awareness outreach campaigns, cybersecurity education and planning resources, threat indicator databases and assistance, and a cybersecurity information sharing network.

<sup>23</sup>National Institute of Standards and Technology's Risk Management Framework, Special Publication 800-37, lists steps to identify organizational cybersecurity risk and to select and implement appropriate security controls. National Institute of Standards and Technology, *Guide for Applying the Risk Management Framework to Federal Information Systems, A Security Life Cycle Approach*, NIST Special Publication 800-37 (Gaithersburg MD, February 2010).

---

See appendix II for a listing of the 15 resources we identified.

While DOD OSBP officials recognized the importance of identifying and disseminating cybersecurity resources through outreach and education efforts to defense small businesses, they also identified a number of factors that had, to date, limited their progress in doing so. Specifically, DOD OSBP officials were not aware of existing cybersecurity resources such as those we identified when we met with them in June 2015, there had been leadership turnover within the office, and the office had been focused on one of its key initiatives—developing the training curriculum for DOD professionals who work with small businesses. OSBP officials also stated that they had been focused on their statutory requirements such as training the DOD workforce that works with small businesses, advocating for small businesses within the government, and reaching out to small businesses in the private sector. While we recognize that these factors could affect progress, federal government internal controls state that management should ensure that there are adequate means of communicating with, and obtaining information from, external stakeholders who may have a significant impact on the agency's achieving its goals.<sup>24</sup> While they had not yet identified or disseminated information about existing cybersecurity resources to defense small businesses, officials agreed that doing so could help the businesses to become more aware of cybersecurity practices and cyber threats. In addition, by identifying and disseminating this information, DOD OSBP could help defense small businesses to protect their networks against cyber exploits, which would support the 2015 DOD Cyber Strategy goals of working with the private sector to help secure defense industrial base trade data and build layered cyber defenses.<sup>25</sup> Furthermore, by identifying existing federal government resources, OSBP's efforts would be in line with DOD Instruction 5134.04, which states that the OSBP Director shall use the existing services and systems of DOD and other federal agencies, when practicable, to avoid duplication and to achieve maximum efficiency and economy.<sup>26</sup> Finally, once OSBP has identified the resources, it can also share them with military department and

---

<sup>24</sup>[GAO/AIMD-00-21.3.1](#).

<sup>25</sup>DOD, *The Department of Defense Cyber Strategy*, April 2015.

<sup>26</sup>DOD Instruction 5134.04 *Director of Small and Disadvantaged Business Utilization* (Sept. 27, 2005).

---

component small business offices so that they can use them for their own outreach and education efforts with defense small businesses.

---

## Conclusions

DOD spends billions of dollars contracting with defense small businesses, and relies on these businesses to support its missions. However, defense small businesses face challenges in protecting their corporate networks and information from increasing cyber threats. While DOD OSBP officials have recognized the importance of educating defense small businesses about cybersecurity, they have not identified and disseminated cybersecurity resources through their outreach and education efforts to businesses because they have been focused on other priorities, such as developing a training curriculum for DOD professionals who work with small businesses. By identifying and disseminating information about existing cybersecurity resources to defense small businesses, these businesses may be made more aware of cybersecurity practices and cyber threats, thereby potentially assisting them in protecting their networks against cyber exploits. By leveraging resources that DOD components and other federal agencies have already developed, some of which have been identified in this report, DOD OSBP will be able to spend more time focusing on other priorities such as developing the training curriculum.

---

## Recommendation for Executive Action

To better position defense small businesses in protecting information and networks from cyber threats, we recommend that the Secretary of Defense direct the Director of the DOD OSBP, as part of its existing outreach efforts, to identify and disseminate cybersecurity resources to defense small businesses.

---

## Agency Comments and Our Evaluation

We provided a draft of this report to DOD, the Federal Communications Commission, the Department of Homeland Security, the Department of Justice, the U.S. Small Business Administration, and the National Institute of Standards and Technology for review and comment.

DOD's written comments are included in appendix III. DOD concurred with our recommendation that the Secretary of Defense direct the Director of the DOD OSBP, as part of its existing outreach efforts, to identify and disseminate cybersecurity resources to defense small businesses. DOD stated that understanding the essential need to protect DOD critical networks, information and infrastructure—including those within defense small businesses—DOD OSBP, with support from the DOD Chief

---

Information Officer, is expanding its current cybersecurity awareness and outreach programs. DOD stated further that the resources we identified reflect a thorough assessment of available federal capabilities and are very helpful to any organization conducting cybersecurity education for its stakeholders. DOD noted that future outreach by the DOD OSBP will increase awareness of cybersecurity education and training resources to defense small businesses. Finally, DOD noted that OSBP will also increase awareness of the cybersecurity education resources among the DOD small business workforce through training events and education programs, and by issuing guidance to the military departments and defense agencies. DOD OSBP added in its technical comments that the office has new leadership and staff in place to expand cybersecurity education for small businesses. The office also noted that it is using a measured approach involving existing information resources and inclusion of cybersecurity information in the development of DOD workforce training and the ongoing creation of outreach materials and presentations. We believe that by identifying and disseminating cybersecurity information, DOD OSBP will help defense small businesses to become more aware of cybersecurity practices and cyber threats and help them protect their networks against cyber exploits.

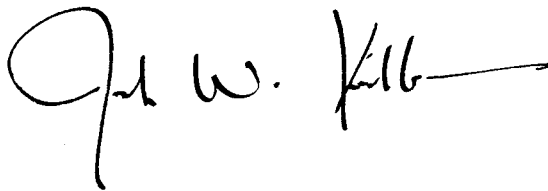
In technical comments on the report, the Federal Communications Commission identified the following additional federal cybersecurity resource—the [Communications Security, Reliability and Interoperability Council - Cybersecurity Risk Management and Best Practices Working Group 4: Final Report](#). The report's appendix provides cybersecurity risk management and best practice recommendations for small and medium business interests, includes potential challenges and barriers to best practice implementation, and includes a compilation of cybersecurity resources available to small businesses. Although the report appendix is intended for small and medium businesses in the communications industry, it is also publicly available online to defense small business contractors.

DOD provided additional technical comments that we incorporated as appropriate. The Department of Homeland Security and the National Institute of Standards and Technology also provided technical comments that we incorporated as appropriate. The U.S. Small Business Administration and the Department of Justice did not comment on the report.

---

We are sending copies of this report to appropriate congressional committees; the Secretary of Defense; the Secretary of Homeland Security; the U.S. Attorney General; the Chairman of the Federal Communications Commission; the Director of the National Institute of Standards and Technology; and the Administrator of the U.S. Small Business Administration. In addition, the report is available at no charge on the GAO website at <http://www.gao.gov>.

If you or your staff have any questions concerning this report, please contact me at (202) 512-9971 or [KirschbaumJ@gao.gov](mailto:KirschbaumJ@gao.gov). Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix IV.

A handwritten signature in black ink, reading "Joe W. Kirschbaum" with a long horizontal flourish extending to the right.

Joseph W. Kirschbaum  
Director, Defense Capabilities and Management

---

# Appendix I: Scope and Methodology

---

We focused our review on the Department of Defense (DOD) Office of Small Business Programs (OSBP) because this office is responsible for providing small business policy advice to the Office of the Secretary of Defense and for providing policy oversight to DOD military department and DOD component small business offices, per DOD Directive 4205.01.<sup>1</sup> While other DOD components such as the DOD Chief Information Officer and military department small business program offices may interact with small businesses, we found these other components either do not exclusively focus their efforts on small businesses or they rely on DOD OSBP policy and guidance with regard to working with small businesses.

To address the extent to which the DOD OSBP has integrated cybersecurity into its existing outreach and education efforts for defense small businesses, we analyzed documentation and interviewed officials from the DOD OSBP about its existing cybersecurity outreach and education efforts to small businesses. We also discussed with DOD OSBP officials any challenges or limitations to their ability to conduct cybersecurity outreach and education. As part of this review, we evaluated the office's efforts by comparing information on their activities with *Standards for Internal Control in the Federal Government*.<sup>2</sup>

By reviewing agency websites, interviewing agency officials, and searching literature on cybersecurity resources, we determined that there was no central repository of federal cybersecurity resources that could be leveraged by the DOD OSBP to share with defense small businesses. In the absence of such a central repository, we reviewed documentation and interviewed officials from the following organizations with cybersecurity expertise: DOD Chief Information Officer, Defense Security Service, Defense Information Systems Agency, Department of Homeland Security National Protection and Programs Directorate, Federal Bureau of Investigation Cyber Division, National Institute of Standards and Technology, U.S. Small Business Administration, Federal Communications Commission, and the National Cyber Security Alliance in order to identify examples of existing cybersecurity outreach and education programs potentially available to defense small businesses that could be leveraged by the DOD OSBP. We limited the scope of our

---

<sup>1</sup>DOD Directive 4205.01 *DOD Small Business Programs* (March 10, 2009).

<sup>2</sup>GAO, *Standards for Internal Control in the Federal Government*, [GAO/AIMD-00-21.3.1](#) (Washington, D.C.: November 1999).

research to cybersecurity outreach and education programs that were managed or funded by federal agencies. To confirm that these resources were accessible to defense small businesses, we visited the websites where these resources were publicly available during May 2015 or interviewed agency officials. To validate that the resources were relevant to cybersecurity, we reviewed information on the resource websites to confirm that each resource contained some level of cybersecurity information. We may not have identified all of the resources available or interviewed all knowledgeable parties, and we did not assess the quality of the selected resources.

To describe the approximate size of DOD's current small business community, we aggregated obligations data for DOD's prime contractors coded as small in the Federal Procurement Data System-Next Generation database for fiscal year 2014. This database does not collect data on subcontractors to defense businesses, so the reported data likely underestimate the size of the DOD small business community. We compared this data to the U.S. Small Business Administration Fiscal Year 2014 Small Business Goaling Report and found the data to be sufficiently reliable to provide an overview of DOD's spending on prime contracts with small businesses.<sup>3</sup> We define the terms "cybersecurity" and "threat" in the introduction of the report using definitions from the National Institute of Standards and Technology<sup>4</sup> and we define "small business" in the introduction of the report using DOD's methodology.<sup>5</sup>

We conducted this performance audit from February 2015 to September 2015 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe

---

<sup>3</sup>U.S. Small Business Administration, *Small Business Goaling Report*, Fiscal Year 2014.

<sup>4</sup>NISTIR 7298, Revision 2, *Glossary of Key Information Security Terms*, May 2013.

<sup>5</sup>DOD defines small businesses according to the North American Industry Classification System used by the U.S. Small Business Administration. The North American Industry Classification System assigns codes to economic activity within 20 broad sectors such as Manufacturing, Finance and Insurance, and Educational Services. The codes reflect the industry in which the firm operates, for example wireless telecommunications carriers or industrial building construction.

---

that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

# Appendix II: Federal Government and Federally-Funded Cybersecurity Resources GAO Identified as Available to Defense Small Businesses

**Table 3: Cybersecurity Resources GAO Identified as Available to Defense Small Businesses**

Resource	Implementing agency/organization	Program overview	Audience
<b>Public cybersecurity awareness outreach campaigns.</b> These programs educate organizations about cybersecurity issues such as the cyber threat and cybersecurity best practices.			
<a href="#">Stop. Think. Connect.</a>	Department of Homeland Security National Cyber Security Alliance Anti-Phishing Working Group	Provides cybersecurity awareness resources such as tip sheets and outreach events targeted to various audiences, such as children, parents, and businesses.	Available to the public, with programs targeted to specific audiences, including businesses.
<a href="#">National Cyber Security Awareness Month</a>	Department of Homeland Security, with public and private partners	Private and public entities collaborate each October to raise awareness of cybersecurity issues. The program uses materials from existing cybersecurity awareness and education resources to assist the public. The program's website includes a page for small businesses with tip sheets and cybersecurity guides.	Available to the public, with programs targeted to specific audiences, including small businesses.
<b>Cybersecurity education for risk assessment and planning.</b> These programs provide education and training that small businesses can use to identify areas of cybersecurity risk and improve their cybersecurity practices and plans.			
<a href="#">Information Assurance Support Environment Online Training</a>	DOD Defense Information Systems Agency	Provides training materials on cybersecurity awareness and technical and legal issues related to government network security, cybersecurity for organization leaders, and personal cybersecurity awareness. The cybersecurity awareness training is mandatory for all users of DOD-furnished computers and holders of Common Access Cards.	Available to the public.
<a href="#">Center for Development of Security Excellence Cybersecurity e-Learning Courses</a>	DOD Defense Security Service	Provides or links users to online courses related to cybersecurity topics such as computer safety and DOD certification and compliance requirements.	Some resources available to the public.

**Appendix II: Federal Government and  
Federally-Funded Cybersecurity Resources  
GAO Identified as Available to Defense Small  
Businesses**

<b>Resource</b>	<b>Implementing agency/organization</b>	<b>Program overview</b>	<b>Audience</b>
<a href="#">Cyber Resilience Review</a>	Department of Homeland Security Office of Cybersecurity and Communications	A self-assessment tool that businesses can use to evaluate their cybersecurity measures. The Cyber Resilience Review website also includes a guide to compare security practices to the National Institute of Standards and Technology's cybersecurity framework. <sup>1</sup> Businesses can also request for the Department of Homeland Security to facilitate the review.	Intended for business cybersecurity (available to the public).
<a href="#">National Initiative for Cybersecurity Education</a>	National Institute of Standards and Technology DOD Department of Homeland Security Department of Education National Science Foundation Office of Personnel Management Department of Labor	A national initiative to address cybersecurity education and workforce development through a public-private partnership between government, academia, and the private sector. The program seeks to accelerate learning and skills development, establish a diverse learning community, and enhance workforce development and career planning.	Professional workforce and students from K-12 and higher education.
<a href="#">Small Business Administration Learning Center: Cybersecurity for Small Business</a>	U.S. Small Business Administration	Provides a thirty minute online program that covers cybersecurity concepts for small business. Topics include identifying and securing sensitive information, types of cyber threats, risk management, and best practices for guarding against cyber threats.	Targeted to small businesses (available to the public).

<sup>1</sup>National Institute of Standards and Technology's Risk Management Framework, Special Publication 800-37, lists steps to identify organizational cybersecurity risk and to select and implement appropriate security controls. National Institute of Standards and Technology, *Guide for Applying the Risk Management Framework to Federal Information Systems, A Security Life Cycle Approach*, NIST Special Publication 800-37 (Gaithersburg MD, February 2010).

**Appendix II: Federal Government and  
Federally-Funded Cybersecurity Resources  
GAO Identified as Available to Defense Small  
Businesses**

<b>Resource</b>	<b>Implementing agency/organization</b>	<b>Program overview</b>	<b>Audience</b>
<a href="#">Small Business Community Computer Security Workshops</a>	National Institute of Standards and Technology, U.S. Small Business Administration, Federal Bureau of Investigation	Workshops on cyber threats, data vulnerability, and security practices. A U.S. Small Business Administration official stated that there are usually 10 to 15 workshops per year, with 50 to 100 participants at each workshop.	Small businesses, local government, educators, non-profit organizations.
<a href="#">NIST Computer Security Resource Center</a>	National Institute of Standards and Technology	Provides reference and training materials on cybersecurity issues, including the interpretation and implementation of the National Institute of Standards and Technology's Risk Management Framework. The site also features a Small Business Corner page that presents a threat awareness video, network security assessment exercises, presentation materials for the Small Business Community Computer Security Workshops, and a National Institute of Standards and Technology Interagency Report on small business information security. <sup>2</sup>	Targeted to small business (available to the public).
<a href="#">Federal Communications Commission Small Biz Cyber Planner 2.0</a>	Federal Communications Commission	Provides guidance based on a small business's self-identified areas of risk. The guidance includes links to additional cybersecurity resources for small businesses.	Targeted to small business (available to the public).

<sup>2</sup>NIST, *Small Business Information Security: The Fundamentals*, NISTIR 7621 (Gaithersburg MD, October 2009).

Appendix II: Federal Government and  
Federally-Funded Cybersecurity Resources  
GAO Identified as Available to Defense Small  
Businesses

Resource	Implementing agency/organization	Program overview	Audience
<b><u>Threat indicator databases and assistance.</u></b> These programs provide threat indicators to help organizations detect and block cybersecurity threats.			
<a href="#">Defense Industrial Base Cyber Security/Information Assurance Program</a>	DOD Chief Information Officer	Provides members with more than 117,000 unclassified threat indicators, including technical signatures that identify potentially malicious actors. Defense Industrial Base Cyber Security/Information Assurance also includes a classified explanation for each threat indicator. Additionally, Defense Industrial Base Cyber Security/Information Assurance members receive regular updates on new threats, and receive additional assistance as needed from DOD Chief Information Officer based on information collected by DOD. Defense Industrial Base Cyber Security/Information Assurance also provides an environment for threat information sharing among members through regular threat information updates and actions as needed from the DOD Chief Information Officer based on information provided by Defense Industrial Base Cyber Security/Information Assurance members.	Defense Industrial Base Cyber Security/Information Assurance is open to defense contractors with a National Industrial Security Program Facility Security Clearance with approved safeguarding for at least Secret information and a Communication Security account with access to DOD secure transmission systems.
<a href="#">Cyber Information Sharing and Collaboration Program</a>	Department of Homeland Security Office of Cybersecurity and Communications	The Cyber Information Sharing and Collaboration Program Operations Team hosts analyst-to-analyst technical threat exchanges, analyst teleconferences and analyst training events that allow for classified and unclassified briefings. They include government and industry partners sharing details of cyber threat activity, and mitigation recommendations and strategies.	Company membership and membership through Information Sharing and Analysis Centers available to critical infrastructure businesses, including defense contractors.

**Appendix II: Federal Government and  
Federally-Funded Cybersecurity Resources  
GAO Identified as Available to Defense Small  
Businesses**

Resource	Implementing agency/organization	Program overview	Audience
<a href="#">Enhanced Cybersecurity Services</a>	Department of Homeland Security Office of Cybersecurity and Communications	Provides classified and unclassified threat indicators from Department of Homeland Security intelligence to internet commercial service providers. The Department of Homeland Security shares classified, sensitive, and unclassified cyber threat indicators with commercial service providers. U.S.-based public and private entities then pay the providers to block malicious domains and e-mails.	U.S. public and private entities, including small businesses.
<a href="#">Defense Security Service Counterintelligence Reports</a>	Defense Security Service	Defense Security Service provides annual reports on threats to cleared defense industry activities, and provides individualized threat information assistance to contractors in the National Industrial Security Program with a security clearance.	Contractors in the National Industrial Security Program with a security clearance, with unclassified reports available to the public.

**Information sharing network.** This network enables discussion and sharing of threat information among its members.

<a href="#">InfraGard</a>	Federal Bureau of Investigation	A network for individuals from private industry, academia, the Federal Bureau of Investigation, and other government agencies to share threat information, including cyber threat information.	Individual membership available to U.S. citizens, including those affiliated with small business. InfraGard has more than 80 chapters across the United States.
---------------------------	---------------------------------	--	---

Source: GAO analysis of information from listed agencies. | GAO-15-777

# Appendix III: Comments from the Department of Defense



ACQUISITION,  
TECHNOLOGY  
AND LOGISTICS

## OFFICE OF THE UNDER SECRETARY OF DEFENSE

3000 DEFENSE PENTAGON  
WASHINGTON, DC 20301-3000

Mr. Joseph Kirschbaum  
Director  
Defense Capabilities Management  
U.S. Government Accountability Office  
441 G Street, NW  
Washington DC 20548

SEP 11 2015

Dear Mr. Kirschbaum,

This is the Department of Defense (DoD) response to the GAO Draft Report GAO-15-777, "DEFENSE CYBERSECURITY, Opportunities Exist for DoD to Share Cybersecurity Resources with Small Business," dated August 24, 2013 (GAO Code 352023).

Enclosed is the DoD's proposed response to the subject report. My point of contact is Ms. Wendy Despres who can be reached at [wendy.e.despres.civ@mail.mil](mailto:wendy.e.despres.civ@mail.mil) and phone 571-372-6313.

Sincerely,

A handwritten signature in black ink, appearing to read "Kenyata L. Wesley", is written over a horizontal line.

A small handwritten mark, possibly initials "SW", is written to the left of the typed name.

Kenyata L. Wesley  
Acting Director, Office of Small Business Programs

Enclosure:  
As stated

GAO DRAFT REPORT DATED AUGUST 24, 2015  
GAO-15-777 (GAO CODE 352023)

**“DEFENSE CYBERSECURITY: OPPORTUNITIES EXIST FOR DOD TO SHARE  
CYBERSECURITY RESOURCES WITH SMALL BUSINESSES”**

**DEPARTMENT OF DEFENSE COMMENTS  
TO THE GAO RECOMMENDATION**

**RECOMMENDATION:** To better position defense small businesses in protecting information and networks from cyber threats, GAO recommends that the Secretary of Defense direct the Director of the DoD OSBP, as part of its exiting outreach efforts, to identify and disseminate cybersecurity resources to defense small businesses.

**DoD RESPONSE:** Concur. Understanding the essential need to protect DoD critical networks, information, and infrastructure including those within defense small businesses, the Department of Defense Office of Small Business Programs (OSBP), with support from the DoD Chief Information Officer (CIO), is expanding its current Cybersecurity Awareness and outreach programs.

The cybersecurity education resources identified in the GAO report reflect a thorough assessment of available federal capabilities and are very helpful to any organization conducting cybersecurity education for its stakeholders. Future outreach by the DoD OSBP will increase awareness of cybersecurity education and training resources to defense small businesses. The DoD OSBP will also increase awareness of the cybersecurity education resources among the DoD Small Business workforce through training events, education programs and by issuing guidance to the Military Departments and Defense Agencies.

---

# Appendix IV: GAO Contact and Staff Acknowledgments

---

## GAO Contact

Joseph W. Kirschbaum, (202) 512-9971 or [KirschbaumJ@gao.gov](mailto:KirschbaumJ@gao.gov)

---

## Staff Acknowledgments

In addition to the contact named above, GAO staff who made significant contributions to this report include Tommy Baril (Assistant Director), Tracy Barnes, David Beardwood, Kevin Copping, and Patricia Farrell Donahue.

---

# Related GAO Products

---

*Information Security: Cyber Threats and Data Breaches Illustrate Need for Stronger Controls across Federal Agencies.* [GAO-15-758T](#). Washington, D.C.: July 8, 2015.

*Insider Threats: DOD Should Strengthen Management and Guidance to Protect Classified Information and Systems.* [GAO-15-544](#). Washington, D.C.: June 2, 2015.

*Cybersecurity: Actions Needed to Address Challenges Facing Federal Systems.* [GAO-15-573T](#). Washington, D.C.: April 22, 2015.

*Information Security: Agencies Need to Improve Oversight of Contractor Controls.* [GAO-14-612](#). Washington, D.C.: August 8, 2014.

*Information Security: Agencies Need to Improve Cyber Incident Response Practices.* [GAO-14-354](#). Washington, D.C.: April 30, 2014.

*Information Security: Federal Agencies Need to Enhance Responses to Data Breaches.* [GAO-14-487T](#). Washington, D.C.: April 2, 2014.

*Federal Information Security: Mixed Progress in Implementing Program Components; Improved Metrics Needed to Measure Effectiveness.* [GAO-13-776](#). Washington, D.C.: September 26, 2013.

*Government Contracting: Federal Efforts to Assist Small Minority Owned Businesses.* [GAO-12-873](#). Washington, D.C.: September 28, 2012.

*Defense Cyber Efforts: Management Improvements Needed to Enhance Programs Protecting the Defense Industrial Base from Cyber Threats.* GAO-12-762SU. Washington, D.C.: August 3, 2012. This report is restricted to official use only and is not publicly available.

*Information Security: Cyber Threats Facilitate Ability to Commit Economic Espionage.* [GAO-12-876T](#). Washington, D.C.: June 28, 2012.

*Cybersecurity: Threats Impacting the Nation.* [GAO-12-666T](#). Washington, D.C.: April 24, 2012.

*IT Supply Chain: National Security-Related Agencies Need to Better Address Risks.* [GAO-12-361](#). Washington, D.C.: March 23, 2012.

---

## GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

---

## Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (<http://www.gao.gov>). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to <http://www.gao.gov> and select "E-mail Updates."

---

## Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <http://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

---

## Connect with GAO

Connect with GAO on [Facebook](#), [Flickr](#), [Twitter](#), and [YouTube](#).  
Subscribe to our [RSS Feeds](#) or [E-mail Updates](#).  
Listen to our [Podcasts](#) and read [The Watchblog](#).  
Visit GAO on the web at [www.gao.gov](http://www.gao.gov).

---

## To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: <http://www.gao.gov/fraudnet/fraudnet.htm>

E-mail: [fraudnet@gao.gov](mailto:fraudnet@gao.gov)

Automated answering system: (800) 424-5454 or (202) 512-7470

---

## Congressional Relations

Katherine Siggerud, Managing Director, [siggerudk@gao.gov](mailto:siggerudk@gao.gov), (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

---

## Public Affairs

Chuck Young, Managing Director, [youngc1@gao.gov](mailto:youngc1@gao.gov), (202) 512-4800, U.S. Government Accountability Office, 441 G Street NW, Room 7149, Washington, DC 20548



Please Print on Recycled Paper.